Community Viewer (CV) 1.5

Deployment, Installation, Backout and Rollback Guide

November 2016

Version 1.1

Department of Veterans Affairs (VA)

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
11/10/2016	1.1	Addressed client comments. Resubmitted	AbleVets
11/03/2016	1.0	Submitted for CLIN 0002BJ, 0002BS	AbleVets
10/11/2016	0.1	Initial draft of document	Apex Data Solutions

Artifact Rationale

This document describes the Deployment, Installation, Backout, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Backout, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

The Community Viewer (CV) is a browser-based software application built on the Joint Legacy Viewer (JLV) system. CV facilitates the secure exchange of data between Veterans Administration (VA) systems and non-VA providers, known as Community Care Providers (CCPs). The exchange of data improves care coordination and continuity of care for VA patients receiving treatment outside of the VA network.

CV pulls information from VA health care systems in real time for viewing within a web browser. Through CV, VA Administrative Staff (VAS) can assign consultations to CCPs and provision CCP use within the CV system, allowing CCPs access to view patient records from multiple VistA systems.

1.1 Purpose

The purpose of this document is to detail the planned installation and deployment procedures for the CV web application and its associated servers and services. The document also identifies resources and a communication plan for deployment-related events.

1.2 Dependencies

Currently, CV is dependent on ancillary services that connect the application to specific data sources. If there are any disruptions with the connections between CV, services, and data sources, the connection(s) may not be available for validation.

CV servers located within the Austin Information Technology Center (AITC) are subject to internal VA update requirements, including database flips, and updates to the servers and security patches performed in VA-controlled data centers. If any of the Enterprise VA operational procedures disrupt the normal operation of CV, the application may not be fully functional.

1.3 Constraints

Physical environments held at the VA AITC, which provide security and environmental control over the CV servers, are restricted by Elevated Privilege (EP) access. Limitations with EP access may impact the ability to respond to issues affecting VA-controlled servers.

1.4 Roles and Responsibilities

Table 1: Roles and Responsibilities

Name	Title/Group	Company
Latricia (Renae) Facundus	Enterprise Program Management Office (EPMO)/ Authorization Approval and Program Manager (PM)	VA
Chad Guebert	Contract PM Lead	AbleVets
Brad Goo	Technical Lead/Application Architect	Hawaii Resource Group (HRG) Technologies LLC

Name	Title/Group	Company
Michael Cardenas	Application Support/Sr. System Engineer, JLV Support Team	HRG Technologies LLC
Gene Sanchez	Enterprise Operations/ Application Manager	Lockheed Martin
Meltron Kendrick	System Administrator/Systems	Technatomy
Jose Negron	System Engineer/Data Center	ByLight

Table 2: Deployment, Installation, Backout, and Rollback Roles and Responsibilities

ID	Team	Phase/Role	Tasks	Project Phase
1	JLV Support	Deployment	Plan and schedule deployment (including orchestration with vendors).	Phase 2
2	JLV Support	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Phase 2
3	JLV Support	Deployment	Test for operational readiness.	Phase 2
4	JLV Support	Deployment	Execute deployment.	Phase 2
5	JLV Support	Installation	Plan and schedule installation.	Phase 2
6	JLV Support	Installation	Ensure authority to operate and that certificate authority security documentation is in place.	Phase 2
7	JLV Support	Installation	Validate through facility Point of Contact (POC) that Information Technology (IT) equipment has been accepted using asset inventory processes.	Phase 2
8	JLV Support	Installation	Coordinate training.	Phase 2
9	JLV Support	Backout	Confirm availability of backout instructions and backout strategy. Identify the criteria that trigger a backout.	Phase 2
10	JLV Support	Post-Deployment	Hardware, Software, and System Support.	Phase 2

2. Deployment

This section provides the schedule and milestones for phased rollout and deployment. Once EPMO approval is granted, the JLV Support team schedules the deployment, in coordination with the VA Production and Data Center team(s). An Automated Notification Request (ANR) is sent to those who will be affected prior to the known effective down time.

Table 3: Implementation Plan Summary

Affected systems and environments	**Component:**	**Deployed to:**
	CV Web Application (for VA Administrative users)	AITC-Enterprise Operation (EO) Cloud Environment
	CV Web Application (for Community Care Provider users)	AITC Non-cloud Environment
	jMeadows Data Service	AITC-EO Cloud Environment
	CV Database	AITC-EO Cloud Environment
	VistA Data Service	AITC-EO Cloud Environment
	CV Quality of Service (QoS)	AITC-EO Cloud Environment
Users impacted by the change	All users of the CV web application	
Estimated timeframe for application deployment	8 hours	
Required pre-implementation work	Authorized users should access the secure repository and download the installation files.	

Compliance standards set by Section 508 of the Rehabilitation Act of 1973, which requires federal agencies to provide software and website accessibility to people with disabilities, are tested and approved prior to delivery of production code. Compliance with 508 requirements will be met by the submission of 508 reports.

2.1 Timeline

The deployment and installation duration is estimated at 2 hours, 30 minutes, as provided above in *Table 3*.

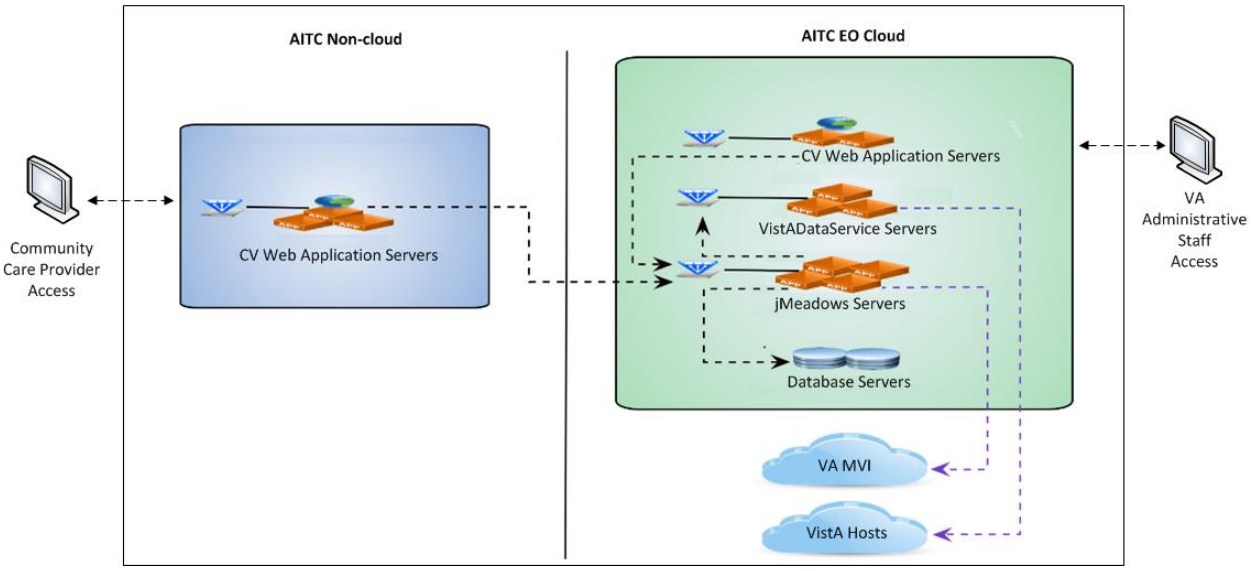
2.2 Site Readiness Assessment

JLV-C servers currently deployed in AITC production environments will be utilized to host the CV web application and its associated services.

2.2.1 Deployment Topology (Targeted Architecture)

Figure 1 below represents the targeted architecture for the CV web application, its associated servers, and associated services.

Figure 1: CV Web Application Deployed in AITC Production Environments



2.2.2 Site Information (Locations, Deployment Recipients)

The VA AITC will host the CV web application and its system components.

2.2.3 Site Preparation

Servers and system components to be utilized by the CV system in the VA AITC should be updated on a regular, scheduled basis with the latest program updates and security patches.

Table 4 describes site preparations required prior to deployment.

Table 4: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
AITC	Security Patches	None identifiable	Implement/Verify	JLV Support
AITC	Program Updates	None identifiable	Implement/Verify	JLV Support

2.3 Resources

The installation and deployment process for CV components residing in the AITC EO Cloud environment is performed and managed by the JLV Support team.

The installation and deployment process for the CV web application residing in the AITC Non-cloud environment is performed and managed by VA Data Center representatives.

Details of the hardware and software utilized within VA production environments are provided in *Table 5* and *Table 6*.

2.3.1 Facility Specifics

The application is deployed at AITC. Details of the hardware and software utilized within VA production environments are provided in *Table 5* and *Table 6*.

2.3.2 Hardware

Table 5 describes the hardware specifications required at each site prior to deployment.

Table 5: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Linux Server	Red Hat Enterprise Linux (RHEL) 6.8	N/A	Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB	Dell	12 Servers for AITC
Database (DB) Server	2012 R2 Enterprise (64-bit)	N/A	Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB	Dell	2 Servers for AITC

2.3.3 Software

Table 6 describes the software specifications required at each site prior to deployment.

Table 6: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
DB Server	N/A	N/A	Microsoft SQL Server 2012 R2	Microsoft (MS)	N/A
Web Application Server	N/A	N/A	Oracle WebLogic Server Version 10.3.6.	Oracle	N/A

2.3.4 Communications

Members of the JLV Support team will perform installation and deployment activities in the EO Cloud environment, and will communicate with the VA Network team, as needed. The CV web application deployment to the AITC Non-cloud environment is performed by AITC. Where possible, installation will be performed during weekends and/or off-hours, so as to minimize the impact on users.

An overview of typical steps and/or communication during the implementation process is as follows:

1. Submit CV release notification.
2. Plan system downtime and change notifications:

a. Veterans Health Administration (VHA) team updates CV newsfeed on appropriate forums.

b. CV PM and OIT PM are notified.

c. Submit EO Request for Change Order (RFCO) for web application deployment in Non-cloud environment:

i. E-mail RFCO form and upgrade documentation to VA IT SDE EO EAS HAS GTD Sustainment group (eashasgtdsustainment@va.gov). Include requested date and time of installation activities on RFCO form.

ii. Approval received from AITC Service Delivery Engineering (SDE) and date/time confirmed.

iii. AITC sends approval request to the PM.

iv. The PM approves request.

3. Back up systems and/or current deployment (to be performed for future releases).
4. Perform installation/deployment:
    a. Current installation removed from service (to be performed for future releases).
5. Validate installation:
    a. Verify EO Cloud installation.
    b. Verify Non-cloud installation.
6. Notification that systems are online:
    a. Notify Product team and users.

2.3.4.1 Deployment/Installation/Backout Checklist

Table 7: Deployment/Installation/Backout Checklist

Activity	Day	Time	Task Owner
Deploy	Saturday	5:00 a.m. EST, with an expected completion time of 1:00 p.m. EST.	JLV Support
Install	Saturday	5:00 a.m. EST. With an expected completion time of 1:00 p.m. EST.	JLV Support
Backout	As needed	As needed, with an expected eight (8) hour completion time.	JLV Support

3. Installation

3.1.1 Pre-installation and System Requirements

Pre-installation and system requirements are specified in *Section 2.3, Resources*.

3.1.2 AITC Coordination

Please see *Section 2.3.4, Communications*, for detailed information regarding coordination with AITC.

3.2 Platform Installation and Preparation

Details of the hardware and software utilized within VA Production environments are provided in *Table 5* and *Table 6*.

3.3 Download and Extract Files

The following list represents planned installation files. The complete file list and file names are subject to final package delivery.

- CV-1.5-update.sql
- CV-CCP-1.5-production.war
- CV-VAS-1.5-production.war
- CVQoS-1.5-production.war
- CVjMeadows-1.5-production.war
- CVVistaDataService-1.5-production.war

3.4 Database Creation

The CV database is a Structured Query Language (SQL) Server 2012 database used for storing community provider account information, patient assignments to community providers, user profile information, and audit records.

Please refer to the CV System Design Document (SDD), provided with product documentation deliverables, for an overview of the CV database design, and a list of database tables.

3.5 Installation Scripts

Installation scripts are not utilized to install the CV web application or its services. The application is installed manually.

3.6 Cron Scripts

Cron scripts are not utilized to install the CV web application or its services.

3.7 Access Requirements and Skills Needed for the Installation

Knowledge of the components and services within the CV application are required for installation and deployment activities. Elevated permissions, or other access requirements, are needed when working within AITC.

3.8 Installation Procedure

The following steps will be performed by the JLV Support team, with the exception of the installation of the CV web application component for deployment in the AITC non-cloud environment.

1. Create a backup of the currently deployed CV system:
    a. Generate Virtual Machine (VM) snapshots for each of the production servers.
    b. Generate a backup of the CV Database by copying the following files:
        i. CV.mdf
        ii. CV_log.ldf
    c. Create copies of the .mdf and .ldf files generated in Step b, and copy the files to a separate directory that can be easily accessed later, if needed.
    d. For reference, record the CV software version number to be installed, as well as the software version number of the previous installation.

Note: Should any problems arise from the deployment of the updated CV system, the backup snapshots and database files will be used to back out of the deployment and restore the previous CV installation.

2. Update the CV database in AITC-EO cloud environment (15-minute time estimate).
    a. Remote desktop into vaausgtdsql200 server.
    b. Open Microsoft SQL Server Management Studio.
    c. Run the SQL Script "CV-1.5-update.sql".
    d. Repeat steps a-c on vaausgtdsql201, the backup database server.
3. Install jMeadows in AITC - EO Cloud environment (30-minute time estimate).
    a. Remote desktop into vaausgtdappprd10 server.
    b. Upload the *jMeadows-[CV version]-production.war* build to *D:\builds* directory on vaausgtdappprd10 server.
    c. Previously deployed *jMeadows-[previous installation]-production.war* build remains as a backup in the *D:\builds* directory.
    d. Open properties file of previously deployed jMeadows war file, validate all endpoints.
    e. Validate all external endpoints are available by testing network connectivity through telnet utility.
    f. Validate all external endpoint web services are available by testing connectivity through web browser on jMeadows servers.
    g. Ensure endpoints in properties file of the new build file match endpoints from the previous build:
        i. VISTA_URL = https://vaausgtdvapprd44.aac.va.gov/VistaDataService/VistaDataService?wsdl

ii. MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService

iii. JNDI_JDBC = jdbc/JanusSQL

iv. JNDI_JDBC_ENCRYPTED = jdbc/JanusSQLTDE

v. RPC_ENDPOINT_ENVIRONMENT = enterprise

h. Log in to the WebLogic Server Administration Console on vaausgtdappprd10 server.

i. Undeploy previously deployed jMeadows-[previous installation]-production.war build.

j. Deploy the jMeadows-[CV version]-production.war build from D:\builds\ directory to the jMeadows cluster. WebLogic distributes the .war file to the clustered servers (vaausgtdappprd10, vaausgtdappprd11, vaausgtdappprd12, vaausgtdappprd13) and stages it in the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

k. Modify deployment configuration to use /jMeadows context root.

l. Start application.

m. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

n. Validate jMeadows endpoint web service is available by testing connectivity through web browser on jMeadows servers.

4. Install CV Web Application for VAS users in AITC-EO cloud environment (30-minute time estimate).

a. Remote desktop into vaausgtdwebprd14 server.

b. Upload the CV-VAS-[CV version]-production.war build to D:\deployable\ directory on vaausgtdwebprd14 server.

c. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

i. If unavailable, open properties file of previously deployed JLV war file and validate jMeadows endpoint.

d. Validate all jMeadows web service is available by testing connectivity through web browser on CV web servers.

e. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

i. grails.jmeadowsURL = https://vaausgtdvapprd43.aac.va.gov/jMeadows/JMeadowsDataService

f. Log in to the WebLogic Server Administration Console on vaausgtdwebprd14 server.

g. Undeploy previously deployed CV-VAS-[previous installation]-production.war build.

h. Deploy the CV-VAS-[CV version]-production.war build from D:\builds\ directory to the CV cluster. WebLogic distributes the .war file to the clustered servers (vaausgtdwebprd14, vaausgtdwebprd15) and stages it in the directory path ${JLV_DOMAIN}\servers\${SERVER_NAME}\stage.

i. Modify deployment configuration to use /CV context root.

j. Start application.

k. Validate CV endpoint is available by testing network connectivity through telnet utility.

l. Validate CV web portal is available by testing connectivity through web browser outside of the CV servers using the public URL.

5. Install CV Web Application for CCP users in AITC Non-cloud environment (30-minute time estimate).

    a. Remote desktop into vaausgtbwebprd10 server.

    b. Upload the CV-CCP-[CV version]-production.war build to D:\deployable\ directory on vaausgtbwebprd10 server.

    c. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

        i. If unavailable, open properties file of previously deployed CV-CCP war file and validate jMeadows endpoint.

    d. Validate all jMeadows web service is available by testing connectivity through web browser on CV web servers.

    e. Ensure endpoints in properties file of the new build file match endpoints from the previous build.

        i. grails.jmeadowsURL = https://vaausgtdvapprd43.aac.va.gov/jMeadows/JMeadowsDataService

    f. Log in to the WebLogic Server Administration Console on vaausgtbwebprd10 server.

    g. Undeploy previously deployed CV-CCP-[previous installation]-production.war build.

    h. Deploy the CV-CCP-[CV version]-production.war build from D:\builds\ directory to the CV cluster. WebLogic distributes the .war file to the clustered servers (vaausgtbwebprd10, vaausgtbwebprd11, vaausgtbwebprd12) and stages it in the directory path ${JLV_DOMAIN}\servers\${SERVER_NAME}\stage.

    i. Modify deployment configuration to use /CV context root.

    j. Start application.

    k. Validate CV endpoint is available by testing network connectivity through telnet

utility.

l. Validate CV web portal is available by testing connectivity through web browser outside of the CV servers using the public URL.

6. Install VistA Data Service in AITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into vaausgtdappprd14 server.
    b. Upload the VistaDataService-[CV version]-production.war build to D:\builds\ directory on same server.
    c. Open properties file of previously deployed Vista Data Service war file, validate all endpoints.
    d. Validate that external endpoints are available by testing network connectivity through telnet utility.
    e. Validate that external endpoints are available by testing connectivity through web browser on Vista Data Service servers.
    f. Log in to the WebLogic Server Administration Console on vaausgtdappprd14 server.
    g. Undeploy previously deployed VistaDataService-[previous installation]-production.war build.
    h. Deploy the VistaDataService-[CV version]-production.war build from D:\builds\ directory. WebLogic distributes the .war file to the clustered servers (vaausgtdappprd14, vaausgtdappprd15, vaausgtdappprd16) and stages it in the directory path ${JLVVDS_DOMAIN}\servers\${SERVER_NAME}\stage.
    i. Modify deployment configuration to use /VistaDataService context root.
    j. Start application.
    k. Validate that VistA Data Service endpoint is available by testing network connectivity through telnet utility.
    l. Validate that VistA Data Service endpoint is available by testing connectivity through web browser on Vista Data Service servers.
7. Install CV QOS Service in AITC-EO Cloud environment (15-minute time estimate).
    a. Remote desktop into vaausgtdappprd10 server.
    b. Upload the CVQOS-[CV version]-.war build to D:\builds\ directory on vaausgtdappprd10 server.
    c. Ensure endpoints in properties file of the new build file match endpoints from the previous build.
        i. ENV = AITC
        ii. JMEADOWS_URL = https://vaausgtdvapprd43.aac.va.gov/jMeadows/JMeadowsDataService?wsdl

iii. VISTA_URL = https://vaausgtdvapprd44.aac.va.gov/VistaDataService/VistaDataService?wsdl

iv. MVI_URL = https://services.eauth.va.gov:8443/external/psim_webservice/IdMWebService

v. JNDI_JDBC = jdbc/Janus

vi. RPC_ENDPOINT_ENVIRONMENT = enterprise

vii. SERVICE_MONITOR_TEST_JMDS = TRUE

viii. SERVICE_MONITOR_TEST_MVI = TRUE

ix. SERVICE_MONITOR_TEST_VDS = TRUE

x. EMAIL_HOST = smtp.va.gov

xi. EMAIL_SSL_PORT = 465

xii. EMAIL_FROM = cv@hawaiirg.com

xiii. EMAIL_TO = cvqos@hawaiirg.com

xiv. EMAIL_SRC_SYS = AITC

d. Log in to the WebLogic Server Administration Console on vaausgtdappprd10 server.

e. Undeploy previously deployed CVQOS build.

f. Deploy the CVQoS-[CV version]-production.war build from D:\builds\ directory. WebLogic distributes the .war file to the directory path ${jMeadows_DOMAIN}\servers\${SERVER_NAME}\stage.

g. Modify deployment configuration to use /CVQoS context root.

h. Start application.

i. Validate that CV QoS endpoint is available by testing network connectivity through telnet utility.

j. Validate that CV QoS endpoint is available by testing connectivity through web browser on CV QoS servers.

3.9 Installation Verification Procedure

After completing the Installation Procedure, perform the following steps to validate the installation and deployment.

1. Validate the installation and functionality of all CV applications and services.
    a. Validate that CV application is running.
        i. Test connection to Web Service Description Language (WSDL).
        ii. Validate ability to connect to CV Login page (internal).

iii. Validate ability to connect to CV Login page (external).

b. Validate that QoS application is running.

i. Validate QoS is writing updates to the DB in the QOS_LOGS table.

ii. Validate system status is reporting on CV login page and in application system status (internal).

iii. Validate system status is reporting on CV login page and in application system status (external).

c. Validate that jMeadows application is running.

i. Test connection to WSDL.

a. On a Linux machine, run the wget command to confirm the download of the webservice definition language file (wsdl).

i. *Wget –no-check-certificate https://<hostname>:<port> /jMeadows/JMeadowsDataService?wsdl*

ii. On CV login page (internal), validate system status.

a. jMeadows should not be listed as being down in system status.

b. System status should show a green checkmark.

iii. On CV login page (external), validate system status.

a. jMeadows should not be listed as being down in system status.

b. System status should show a green checkmark.

d. Validate Virtual Disk Service (VDS) application is running.

i. Test connection to WSDL.

a. On a Linux machine, run the wget command to confirm the download of the webservice definition language file (wsdl).

i. *wget –no-check-certificate https://<hostname>:<port> /VistaDataService/VistaDataService?wsdl*

ii. On CV login page (internal), validate system status.

a. VDS should not be listed as being down in the system status.

b. System status should show a green checkmark.

c. Validate user is able to login with VA credentials.

d. Using test patients CHDR 1 and CHDR 2, validate that VA data is populating in the application.

e. Validate that VA Terminology mapping is occurring in supported widgets.

iii. On CV login page (external), validate system status.

a. VDS should not be listed as being down in the system status.

b. System status should show a green checkmark.

c. Validate user is able to login with CCP credentials.

3.10 Notification of Test Results

After completion of the validation and testing steps, results will be provided to the CV Management team, the Integration Agreement (IA) team, and the VA Management team.

If testing/validation has failed:

1. Notify the CV Management Team, IA Team, VA Management Team. Notify the Network Administrators, as necessary.

3.11 System Configuration

Table 8 describes the server configuration for CV production infrastructure, hosted at AITC.

Table 8: CV Server Specifications

Application or Service	Server Specifications
CV Web Application (for VAS users)	Two (2) servers: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago)
CV Web Application (for CCP users)	Three (3) servers: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago)
Vista Data Service	Three (3) servers: - Intel Xeon CPU X7560 @ 2.27GHz, 2261 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago) One (1) server: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago)
jMeadows Service	Four (4) servers: - Intel Xeon CPU X7560 @ 2.27GHz, 2261 MHz, 2 Cores, 2 Logical Processors, 16 GB - Red Hat Enterprise Linux Server release 6.8 (Santiago)
CV Database	Two (2) servers: - Intel Xeon CPU E5-4657L v2 @ 2.40GHz, 2400 MHz, 2 Cores, 2 Logical Processors, 16 GB - Microsoft Windows Server 2012 R2 Standard

3.12 Database Tuning

Database tuning is not applicable at this time, but may become a necessary component of the installation in the future. At such time, database tuning details will be provided.

4. Backout Procedure

Please see *Section 5, Rollback Procedure*, for detailed steps.

5. Rollback Procedure

The following rollback point has been identified as criteria for initiating the backout plan:

- The application becomes unusable

Perform the following steps to uninstall the JLV system and restore the previous installation:

1. Roll back jMeadows in EO Cloud environment.
    a. Remotely connect to vaausgtdappprd10 server.
    b. Log into WebLogic Server Administration Console on vaausgtdappprd10 server.
    c. In the WebLogic Server Administration Console, un-deploy the jMeadows-[CV- version]-production.war build. WebLogic also un-deploys the build from the clustered server(s).
    d. In the WebLogic Server Administration Console, deploy jMeadows-[previous installation]-production.war build located in the builds directory /u01/JLV_HOME/builds. WebLogic also deploy the build to the clustered servers(s).
    e. Start the application.
    f. Validate all external endpoints are available by testing network connectivity through telnet utility.
    g. Validate all external endpoint web services are available by testing connectivity through web browser on jMeadows servers.
2. Roll back CV Web Application for VAS users in AITC - EO Cloud environment.
    a. Remotely connect to vaausgtdwebprd14 server.
    b. Log into WebLogic Server Administration Console on vaausgtdwebprd14 server.
    c. In the WebLogic Server Administration Console, un-deploy the JLV-[JLV version]-production.war build. WebLogic will also un-deploy it from the clustered server(s).
    d. In the WebLogic Server Administration Console, deploy JLV-[previous installation]-production.war build located in the builds directory /u01/JLV_HOME/builds. WebLogic will also deploy it to the clustered server(s).
    e. Start the application.
    f. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.
    g. Validate jMeadows web service is available by testing connectivity through web browser on JLV web servers.
3. Roll back CV Web Application for CPP users in AITC - EO Non-Cloud environment.

a. Remotely connect to vaausgtdwebprd10 server.

b. Log into WebLogic Server Administration Console on vaausgtdwebprd10server.

c. In the WebLogic Server Administration Console, un-deploy the CV-[CV version]-production.war build. WebLogic will also un-deploy it from the clustered server(s).

d. In the WebLogic Server Administration Console, deploy JLV-[previous installation]-production.war build located in the builds directory /u01/JLV_HOME/builds. WebLogic will also deploy it to the clustered server(s).

e. Start the application.

f. Validate jMeadows endpoint is available by testing network connectivity through telnet utility.

g. Validate jMeadows web service is available by testing connectivity through web browser on JLV web servers.

4. Roll back VistA Data Service in AITC-EO Cloud environment.

   a. Remotely connect to vaausgtdappprd14 server.

   b. Log into WebLogic Server Administration Console on vaausgtdappprd14 server.

   c. In the WebLogic Server Administration Console, un-deploy the VistaDataService-[CV version]-production.war build. WebLogic also un-deploys the build from the clustered server(s).

   d. In the WebLogic Server Administration Console, deploy VistaDataService-[previous installation]-production.war build located in the builds directory /u01/JLV_HOME/builds. WebLogic also deploys the build to the clustered server(s).

   e. Start the application.

   f. Validate that external endpoints are available by testing network connectivity through telnet utility.

   g. Validate that external endpoints are available by testing connectivity through web browser on Vista Data Service servers.

5. Recreate JLV Database in AITC-EO Cloud environment (15-minute time estimate).

   a. Remote desktop into vaausgtdsql200.

   b. Recreate the tables of the previous version of the JLV Database using the CV.mdf and CV_log.ldf files backed up during the upgrade.

6. After completing the backout procedure, perform the validation steps in *Section 3.9, Installation Verification Procedure*.

7. If all else fails, restore the servers from VM snapshots taken before the upgrade.